Protection des données

Poullet, Yves

Published in:
Informatique et Gestion

Publication date:
1981

Document Version
le PDF de l'éditeur

DROIT DE L'INFORMATIQUE

Série animée par Alain Bensoussan.

Le but de ce dossier-série est de donner aux utilisateurs un point de vue plus précis et plus concret sur les problèmes juridiques liés à l'informatisation.

Déjà paru :

- **introduction aux problèmes du droit de l'informatique.**

A paraître dans les prochains numéros :

- **normalisation et règles de l'art ;**
- **la preuve en droit de l'informatique ;**
- **la protection des programmes ;**
- **le contrat informatique ;**
- **l'assurance en informatique ;**
- **la sous-traitance en informatique.**

Protection des données : normes et principes

par Yves POULLET
Faculté des Sciences Economiques et Sociales de Namur

La protection de données constitue un double problème. En effet, être fiché c'est risquer de se trouver en " liberté diminuée ", mais la constitution de fichiers est devenue une nécessité du fonctionnement social. Il faut donc dépasser les réflexes de crainte et s'orienter vers la recherche de normes claires qui permettraient d'équilibrer le droit des organisations à l'information et celui des individus à la liberté.

La notion de " protection des données " est ambiguë. **Elle désigne à la fois la " sécurité " et la " confidentialité ".** L'aspect technique " sécurité des données " n'est qu'un élément infime de la question bien plus complexe de la " confidentialité " c'est-à-dire **du contrôle de l'exercice du libre pouvoir de disposer de l'information personnelle d'autrui.**

Certes, la question de la protection des données n'est pas neuve et sa règlementation est ancienne (secret des affaires, secrets administratifs, etc.). L'introduction de l'informatique a cependant, on ne peut le nier, donné à la question une importance sans commune mesure avec la situation passée. L'informatique étend les capacités de mémorisation des données, permet une corrélation, rapide, facile, souple, économique et sur une large échelle des diverses sources d'informations (passage d'un " seuil qualitatif " dans le traitement des données).

Cette constatation a amené certains à concevoir l'informatique comme un " danger a priori " pour la vie privée de l'individu. Progressivement, on s'aperçoit que cette approche purement négative doit céder le pas à une règlementation plus nuancée qui cherche à concilier ou mieux **équilibrer, d'une part, le " juste " droit à l'information des administrations et entreprises, d'autre part, les libertés de l'individu ou plus largement des fichés** (entreprises, associations et personnes physiques).

Ce sont les principes de cet équilibre que diverses législations cherchent à mettre en évidence, ainsi, les législations nationales de Suède, des Etats-Unis, de la RFA, du Canada, de Norvège, du Luxembourg, de la France, du Danemark, etc. Remarquons que la plupart de ces ordres juridiques ont compris que les principes de la protection des données devaient être modulés, d'une part, **selon des**

critères régionaux (à cet égard, voir les innombrables législations régionales aux Etats-Unis, Canada, Allemagne, etc.), d'autre part, **selon des critères sectoriels** (le domaine du crédit (Etats-Unis, Canada, Suède), de l'emploi (projet allemand), de la Santé, de la Sécurité publique, etc.).

Au-delà de ces règlementations nationales et supranationales, il faut évoquer les travaux directifs ou recommandations d'organismes internationaux (OCDE, CEE, Conseil de l'Europe) qui cherchent à **réglementer les flux transfrontières, et éviter la création de " paradis de données "**, par une harmonisation des législations nationales.

En l'absence d'une législation déjà constituée, c'est une synthèse des divers principes élaborés dans les ordres juridiques nationaux et supranationaux que nous tâcherons d'élaborer.

Nous aurons présent à l'esprit l'impact que ces normes réglementaires peuvent avoir sur la technique et son coût.

Nous étudierons les divers principes sous quatre thèmes :

— principes applicables à la **constitution du " fichier "** ;
— principes applicables au rapport : **fichier-société** ;
— principes applicables au rapport : **fichier-donnée enregistrée** ;
— principes applicables au rapport : **fichier-fiché** (à ce propos, nous étudierons un cas particulier de la responsabilité du ficheur en cas d'erreur dans le traitement des données).

Normes, données et fichiers

La constitution du fichier

Par fichier, nous entendons l'ensemble du réseau informatique interne d'une administration publique ou d'une entreprise (conçue ici comme unité économique minimale indépendamment de sa forme juridique).

Deux grands principes doivent régir la constitution d'un fichier, celui du non-secret et celui de l'auto-responsabilité. Examinons les tour à tour.

Le principe du non-secret signifie que le public doit connaître l'existence de chaque fichier et être sans cesse informé sur toute modification de son fonctionnement. Pour réaliser cette exigence, on peut proposer d'attribuer à tout fichier une " carte d'identité " qui spécifiera ses caractéristiques. Sur ces cartes seront, par exemple, répertoriés les noms et emplacements du système, son responsable légal, le type de traitement effectué, les catégories d'utilisateurs et les buts poursuivis par eux, les catégories d'individus enregistrés et les moyens mis à leur disposition pour exercer leur droit d'accès aux informations les concernant. D'autres rubriques, entre autres, touchant à la politique de stockage et de classement des enregistrements ou encore aux catégories de sources (Privacy Act, USA), devront figurer sur ces cartes qui seront tenues à la disposition de tous dans un " registre public ".

Le principe de l'auto-responsabilité est déjà explicitement avancé par toutes les législations existant en la matière. Il prévoit la nomination par les autorités détentrices du fichier, **d'un responsable à la protection des données.** Cette personne est chargée de veiller à l'application des prescriptions légales sur la protection des données, au respect des divers codes éthiques et déontologiques propres à la profession d'informaticien et, plus largement, au traitement des données. Pour le moment, l'impact de cette obligation légale sur l'organigramme des entreprises est encore peu visible.

Il faut ajouter que toutes les législations reconnaissent que les seuls principes éthiques et déontologiques ne peuvent suffire à assurer une protection valable des données.

Le rapport fichier-société

• **Principe du contrôle sociétaire par la création d'une commission administrative.**

Toutes les législations créent un organisme chargé du contrôle des banques de données. Cet organisme relève de l'autorité tantôt du législatif, tantôt de l'exécutif et remet un rapport annuel public. Il émet des avis sur le développement de l'informatique, son impact sur les libertés individuelles et les principes constitutionnels étatiques.

Une question légitime se pose : l'appel ainsi fait à une lourde artillerie, juridique, administrative et technique, pour la prévention de tous les dangers de l'informatique ne risque-t-elle pas d'amener la formation d'un lobby de techniciens dont l'action serait à son tour difficilement contrôlable par le public, ce qui serait le contraire du but recherché.

• **Principes d'un degré de contrôle a priori, fonction du type de fichier**

Les dernières législations admettent que les **mesures de contrôle a priori,** soient plus ou moins sévères suivant les dangers particuliers présentés par les différents types de fichiers.

Dans des pays comme la RFA, l'Autriche, les Etats-Unis, la Norvège, le Danemark, on distingue le plus fréquemment trois types de fichiers :
— les fichiers publics ;
— les fichiers privés pour compte propre (travaillant dans le cadre d'une relation contractuelle avec le fiché) ;
— les fichiers privés pour compte de tiers (les agences de renseignements commerciaux, les " chercheurs de têtes ", etc.).

Si les fichiers publics doivent faire l'objet d'un contrôle (par voie d'avis ou d'autorisation) lors de leur création (respect des principes constitutionnels, en particulier de l'équilibre des pouvoirs et des libertés publiques des citoyens), la simple déclaration d'existence suffit pour les fichiers du second type. Les fichiers du troisième type sont réglementés et font souvent l'objet d'une autorisation.

• **Principe du contrôle de fonctionnement**

On reconnaît un large pouvoir d'enquête et de surveillance au Comité de contrôle (accès dans les locaux, inspection des bandes magnétiques, vérification des normes de sécurité, etc.).

Cet organisme de contrôle sert de véritable médiateur auprès du public. Certaines législations lui reconnaissent un droit de sanction ou de réglementation (addition de nouvelles normes de sécurité, retrait d'une autorisation, etc.).

Le traitement de la donnée

Par donnée, certaines législations n'entendent que les données " personnes physiques " ; actuellement, sont généralement comprises et les données " personnes physiques " et les données " personnes morales " (entreprises, organisations diverses).

Par " donnée nominative ", il faut entendre " toute information qui directement ou indirectement est rapportable à un individu (une entreprise), une association ou fondation " (définition loi norvégienne) ; ainsi le numéro de registre national est une donnée nominative.

Le principe de la " qualité de la donnée " doit être mis en œuvre pour que les données personnelles utilisées dans un traitement automatique soient exactes, complètes, précises et à jour.

• Pour satisfaire au **principe du caractère exact,** plusieurs points sont à souligner :
— le souhait exprimé d'une prise d'information directe chez le fiché dans toute la mesure du possible ;
— l'obligation faite dans certaines lois, d'indiquer un coefficient de valeur lors de contestations ou de noter la provenance de la donnée dans le cas de données reçues de certains tiers (agences de renseignements commerciaux) ;
— le processus de blocage de la donnée pendant la procédure de vérification (RFA).

Dans l'application de ce principe, il ne faut pas oublier que les données résultant d'une appréciation subjective (dites " données soft ") posent un problème.

• **Le principe de la mise à jour** comporte deux obligations allant de pair :
— l'obligation d'anonymiser ou de bloquer, voire d'effacer certaines données après un certain laps de temps (implication pour l'outil !) ;
— l'obligation de mises à jour fréquentes (Allemagne-Suède par exemple). (Un logiciel permettant cette révision fréquente, devient alors une nécessité.)

• En ce qui concerne **le caractère complet** des informations, il faut bien prendre en compte le droit du fiché à ajouter dans données dans certaines circonstances (par exemple, dans le cas des données relatives au crédit, ce droit existe en Suède, Belgique et en RFA). L'exercice de ce droit devrait atteindre sa plus grande extension lorsqu'il arrive (ce qui est prévu par le " Privacy Act " américain) que, des informations détenues dans le fichier, peuvent découler des conséquences néfastes pour la personne en cause.

• **Principe de la sécurité des données**

Il s'agit de prévenir toute intrusion accidentelle ou intentionnelle non autorisée dans le fichier, toute modification ou tout effacement non voulus. Certes, des mesures techniques sont connues ou possibles mais elles ne sont jamais parfaitement fiables et peuvent être coûteuses, ainsi par exemple, les " systèmes de chiffrement à clef publique ", le " back up ", etc. Les organes de contrôle peuvent prescrire certaines techniques plutôt que d'autres (à cet égard, le choix fait par le National Bureau of Standard (NBS) d'un système de chiffrement peut avoir valeur d'exemple).

On peut citer à ce propos **quelques principes ayant trait à la nécessité et à l'ampleur des mesures de sécurité à prendre** (leur coût variable peut poser des problèmes aux entreprises opposant ainsi nécessité et ampleur).

Le besoin de sécurité dépend de :
— du caractère sensible, du volume et de la fréquence d'utilisation des données enregistrées ;
— des catégories et de la diversité des utilisateurs ;
— de la structure et de l'environnement du système de traitement des données (TURN reprenant les principes affirmés par la commission américaine).

En outre **certains principes de base doivent être respectés.** L'accès, tout d'abord, doit être réservé au seul personnel autorisé c'est-à-dire dont les fonctions requièrent l'utilisation de données qu'elles ont besoin de connaître. La protection physique des enregistrements doit, ensuite, être assurée et la surveillance des communications entre ordinateur et terminaux éloignés (pour empêcher toute possibilité de se brancher sur le réseau) devra être constante. Un ensemble de lourdes sanctions " pénales " est d'ores et déjà disponible pour permettre cette sécurité des données.

Les données enregistrées doivent être " pertinentes ", et ne peuvent être communiquées à des tiers sans

précaution. Le traitement des données ne peut être la source unique d'une décision prise par rapport au fiché.

Principe de la pertinence

La question de la " pertinence " de l'utilisation d'une donnée est certes une des questions les plus difficiles. On peut relever à cet égard différentes règles :

• la pertinence est tantôt appréciée a priori par la commission de contrôle, tantôt ne fait l'objet que d'un contrôle a posteriori lors d'une plainte. Elle est, semble-t-il d'après la plupart des législations, fonction :

— pour les entreprises, traitant pour leur propre compte, de la **finalité du rapport avec le fiché ;**

— pour les administrations publiques, de l'application des **principes de légalité, proportionnalité et spécialité** (Lebrun) ;

— pour les entreprises traitant pour compte de tiers, d'une autorisation préalable ou d'une liberté contrôlée (FCRA américain, Danemark, Norvège) ;

• certaines données sont a priori non pertinentes, les données dites " interdites " ou " à haut degré de sensibilité " (Bing) (race, religion, opinions politiques), d'autres peuvent circuler librement (données dites " neutres " (n° de téléphone, profession, problème de l'identifiant unique !)

On peut donc dire que la pertinence s'apprécie par rapport au but annoncé dès le départ. S'il intervenait une modification de ce but, obligation doit être faite d'avertir, avant de traiter de nouvelles données, les instances compétentes.

Les procédures de **communication** des données requièrent des normes précises.

Il y a communication lorsqu'il y a sortie de l'entreprise ou d'un centre de traitement informatique de l'administration. Cette communication sera soumise à un contrôle multi-critère.

Principe d'un contrôle des communications fonction de leur fréquence.

Plus l'échange d'informations s'intensifie, plus le contrôle sera sévère.

Principe du droit limité à la communication.

Les entreprises ou administrations qui réclament une communication doivent pouvoir faire la preuve d'une non affectation des intérêts du fiché et des exigences de l'utilisation de la donnée pour l'accomplissement de leur fonction (ex. : données réclamées par une société d'assurance à une banque pour la couverture d'un crédit au fiché).

Principe d'un registre des communications

Certaines législations obligent les fichiers qui communiquent à tenir une comptabilité des communications par donnée (implication technique de cette obligation nécessaire pour la rectification d'erreur, le blocage, etc.) et le droit à l'image du fiché.

Principe de la non-suffisance du traitement pour la décision de l'administration ou de l'entreprise

" Aucune décision administrative ou privée impliquant une appréciation sur un comportement humain ne peut avoir pour seul fondement un traitement automatisé d'informations donnant une définition du profil ou de la personnalité de l'intéressé " (art. 2 Loi Française). Ce principe a une grande importance pour le secteur bancaire.

Fichier, ficheur, fiché

Le rapport " fichier-fiché " se construit autour de deux principes : celui du droit à l'image dans le chef du fiché, celui de la responsabilité du ficheur vis-à-vis de ce droit du fiché.

Principe du " droit à l'image ".

Sont bénéficiaires de ce droit à l'image, les fichés personnes physiques et les personnes morales (questions : le droit au " goodwill " des entreprises ne risquent-ils pas de porter atteinte au secret légitime des affaires ?).

Le " droit à l'image " **n'est pas le droit de propriété sur l'image** mais le droit de savoir pourquoi on m'interroge. (Faut-il voir une exception dans la loi française : le fiché peut refuser pour des raisons légitimes l'enregistrement d'une donnée par un fichier).

Le " droit à l'image " est **le droit de connaître la banque de données où je suis enregistré** (comment ? cela engage la responsabilité du ficheur). On peut légitimement se poser une question sur les limites de ce droit qui se définissent comme le problème de connaître les données et/ou l'information-résultat, la source (RFCA américain et suédois), le but du traitement, les raisonnements utilisés (France), les communications.

Les exceptions à ce droit (Police, Défense nationale) sont rares.

Le droit à l'image est le **droit de contester, de compléter de faire effacer une donnée erronnée, incomplète, enregistrée illicitement ou non pertinente.**

Principe de la " responsabilité du ficheur "

Il incombe au ficheur de prévoir les procédures facilitant l'accès des individus (loi américaine : obligation de prévoir un accès direct des fichés à leurs propres " enregistrements " et l'entretien avec le responsable du fiché et de **faire connaître** aux fichés certaines caractéristiques du traitement et les données enregistrées les concernant).

Les modalités pratiques de cette obligation sont variées et peuvent prendre la forme soit d'une notification obligatoire (ce cas est rare), soit d'une notification à la demande (cas des fichiers d'emploi dans la loi américaine, obligation de prévenir dès la demande d'un tiers).

Le coût de cet accès est variable et est, en général, supporté par le fiché (dans des limites précises) et par le ficheur (décret allemand du 22 décembre 1977, par exemple).

En ce qui concerne **la forme** de l'accès du fiché aux informations elle doit être lisible et rédigée dans un langage compréhensible pour lui non spécialiste. **Obligation est faite également de ne rien dissimuler** (le fiché a droit de recours auprès des autorités juridictionnelles pour faire vérifier si tous les renseignements sur la personne fichée lui ont été délivrés. L'organe de contrôle doit éventuellement lui apporter son concours).

Le ficheur est, enfin, **obligé de rectifier, compléter, bloquer et de faire rectifier, compléter ou bloquer auprès des tiers** les données devenues erronées. (Les procédures internes à l'administration ou à l'entreprise sont généralement prévues dans un premier temps avant le recours aux autorités juridictionnelles.)

L'impact technique de ce principe est important. Sa première conséquence est la nécessité pour les fichiers de pouvoir sortir à tout moment les données et utilisations de ces données (surtout les communications) relatives à un fiché.

L'évaluation du coût de la responsabilité du ficheur sur ce point précis peut être chiffrée à 25 % du coût global entraîné par les diverses prescriptions de la loi de protection des données. ■

ANNEXE

Textes de lois (les plus significatives) :

— Autriche : Datenschutzgesetz, 18 octobre 1978 ;

— Conseil de l'Europe ; Convention pour la protection des individus, octobre 1980 ;

— Danemark : Loi danoise n° 294 sur les registres publics, 8 juin 1978 ; Loi danoise n° 293 sur les registres privés, 8 juin 1978 ;

— France : Loi n° 78-17 du 6 janvier 1978 : Informatique, Fichiers et Libertés ;

— Luxembourg : Loi du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques ;

— Norvège : Loi du 9 juin 1978 sur les registres de personnes ;

— Suède : Loi du 11 mai 1973 (amendée le 1 juillet 1979) Data Act ; Fair Credit Reporting Act 1973 ;

— République fédérale Allemande : Bundesdatenschutzgesetz, 27 janvier 1977 ;

— USA : Privary Act 31 décembre 1974 ; Fair Credit Reporting Act 1970.